FAX

To: **Commissioner for Patents**
USPTO
P. O. Box 1450
Alexandria, VA 22313-1450
Tel: (703)
Fax: (703) 872-9306
Email:

From: Ajit K. Zacharias
32 Merlin Drive
Brampton, ON L6P1G1
Canada
Tel: (905) 794-2752
Fax: (905) 794-1411
Email: ajitzac@rogers.com

Date: April 5, 2004

This fax contains 38 pages (including this page)

Re: Patent Application 10/089,756

Here is a form (PTO-2038) and 3 copies of an Appeal Brief (12 pages each) pertaining to a Notice of Appeal filed February 6, 2004. Thank you.

32 Merlin Drive, Brampton, ON, L6P 1G1, Canada
Tel: (905) 794-2752 – Fax: (905) 794-1411
Email: ajitzac@rogers.com

April 2, 2004

Applicant	:	Ajit K. Zacharias
Appl. No.	:	10/089,756
I.A. Filing Date	:	October 4, 2000
Priority Date	:	October 15, 1999
Title	:	Secure Multi-Application Card System
Grp. Art Unit	:	2876
Examiner	:	Mr. Seung H. Lee
Docket No.	:	AZSI-P-010

Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Re: Appeal Brief pertaining to Notice of Appeal filed February 6, 2004

Dear Sir/Madam:

This Appeal Brief is submitted in support of my Notice of Appeal filed February 6, 2004 in response to the Office Action of November 17, 2003. I attach the form PTO-2038 authorizing payment of the fee of $ 165.00 (small entity) for filing a brief in support of an Appeal.

If you have any questions, kindly contact me by phone at (905) 794-2752, or email me at ajitzac@rogers.com. Thank you.

Sincerely,

A. K. Zacharias

Ajit K. Zacharias
Sole Inventor and Applicant

APPEAL BRIEF

1. REAL PARTY OF INTEREST:

The Applicant. Not represented by a registered practitioner.

2. RELATED APPEALS AND INTERFERENCES:

None.

3. STATUS OF CLAIMS:

Claims 1-27, 31, 33, 34, 37-43 and Claim 53 were previously cancelled.

Claims 28-30, 32, 35, 36 and 44-52 were previously amended.

4. STATUS OF AMENDMENTS:

No amendments filed subsequent to final rejection.

5. SUMMARY OF THE INVENTION:

The invention is a multi-application card (MAC) system for providing card owners secure access to multiple card (and other) accounts. Since each account could involve access to a different application, it is termed a multi-application card.

A number of attempts have been made to implement a multi-application card system. A major difficulty with implementing such a system is that introducing a completely different hardware technology to implement a multi-application card system would necessitate changing the entire global equipment infrastructure for card processing, making it infeasible. That difficulty is overcome by the present invention. In this invention, a standard magnetic-stripe, smart or bar-coded card is used to access a database containing multiple account numbers, each identified by a unique index number (or code). This allows a MAC owner to carry one card but have use of multiple cards that s/he needs to carry for financial or non-financial applications.

The system comprises a MAC (with a machine-readable number corresponding to the MAC), a database (ideally located remote from the card) and a translator that uses the database to convert the MAC number to the account number the owner wishes to use.

The database correlates the MAC number with a record containing a list of card account numbers, each having a unique index number associated with it. The translator receives a request to convert the MAC number (read from the multi-application card) to the account number, using a manually entered index number (also called a Card Identification Number or CIN). The translator uses the received MAC number to access the corresponding record in the database. **Because each account number is assigned a unique index number within the record,** the translator is able to use the received index number to immediately identify and retrieve the corresponding account number and its associated security information, e.g. expiry date.

To avoid confusion in terminology such as "MAC Number", "Index Number", "PIN", "Card Identification Number" and "Account Number", here are the definitions of terms used in my application and the explanation:

Each Multi-Application Card (MAC) has a number. This is referred to in the following explanation as a "MAC number". The MAC number is read from the MAC by a card reader device.

Each MAC number corresponds to a record in the database. Each record in the database contains sub-records. Locating a specific sub-record in the database requires the MAC Number (to identify the record) and an Index Number (also referred to as a Card Identification Number or CIN) to identify the sub-record within it. The Index Number, typically a 4-digit number, is physically entered at a data entry device such as a keypad.

Most credit and debit card users are familiar with the use of a Personal Identification Number (PIN), which has served to verify the owner of a debit card. A PIN is also typically a 4-digit number, physically entered at a data entry device such as a keypad. Card industry research shows that over 90% of card owners use the same PIN for ALL their Debit, Check, ATM and Convenience cards. This seems logical because a PIN identifies the person, not the card. Credit cards are verified by signature and do not use PINS, making them more prone to fraudulent use.

My invention identifies three categories of index numbers, based on the content of the sub-records they relate to. Within the record, each sub-record identified by index numbers referred to as a "first subset" of index numbers, contains (or points to) a single account number. The account number could be a credit card number, a debit card number, driver's license number, etc. Within the same record, each sub-record identified by index numbers referred to as the "second subset" of index numbers, contains (or points to, or functions as) a LOCK code instead of an account number. Within the same record, each sub-record identified by index numbers referred to as the "third subset" of index numbers, contains (or points to, or functions as) an UNLOCK code, instead of an account number or a LOCK code.

Here are the steps involved in using my invention:

1. The multi-application card (MAC) is read at a card reader. The card reader reads the MAC number.

2. As when using a debit card, the user is asked to physically enter a number in the keypad. The user manually enters a number (called an Index Number or Card Identification Number).

3. The MAC Number and the Index Number are sent from the point-of-service to the card translator system. Using the MAC number, the translator locates a record in its database. The index number (or Card Identification Number) is used to find a sub-record (or entry) within the record. If, as the claim reads, the index number is within the *first* subset of index numbers (i.e. the sub-record identifies or contains a single account number), *that* account number is retrieved and processing continues. The account number could be a credit card number, a debit card number or some other account number. If the index number is within the *second* subset of index numbers (i.e. the sub-record identifies or contains a Lock code instead of an account number), the entire record is flagged as "locked" or "disabled". The MAC can no longer be used to access an account number from the database until the lock flag is removed. If the index number is within the *third* subset of index numbers (i.e. the sub-record identifies or contains an Unlock code instead of an account number or Lock code), the Lock flag for the record is removed, effectively "unlocking" or "re-enabling" the MAC.

The translator then transmits the card account number and other security information back to the sub-system, or program, that requested the translation of the MAC number to the actual account number. Although, in the preferred embodiment, the database and translator reside remote from the card, they could reside on the MAC, within the client subsystem, at the card issuer's system or any point within the network that makes up the Client-Server system.

6. ISSUES:

The Examiner rejects my claim that the PIN in the Rose invention (US 5,770,843) and the CIN in my invention are different. The difference in PIN and CIN, the processing steps and the resulting improvements are readily recognized by those ordinarily skilled in the art as well as Examiners at the European Patent Office and the Canadian Intellectual Property Office, which have granted me patents EP 1221144, and CA 2,381,807 respectively. For some reason the Examiner at the USPTO does not accept the difference. For instance, Claims 28c and 50c specifically claim sufficiency of the MAC Identification Number and the Index Number to identify a single account number. This is neither possible nor claimed in the ROSE invention, yet these claims have been rejected.

I applied for patents at the USPTO in two forms, directly and through the PCT. When the direct US patent was granted, I was compelled to accept narrow claims or have the entire patent denied; I accepted the narrow claims, because I felt I could explain the difference better during the US National Phase of my PCT application with the additional evidence of improvements on the basis of recognition by Examiners in the PCT countries. The narrow claims leave the patent vulnerable to infringement by minor variations. I do not believe this was the intention of the founding fathers of the United States when they instituted the concept of patents. It runs totally counter to the spirit of US Patent Law.

7. GROUPING OF CLAIMS:

Claims 28-30 and 50-52 rejected under U.S.C. 103(a) as being unpatentable over Rose et al (US 5,770,843 of record).

Claims 32, 35, 36 and 45-49 rejected under U.S.C. 103(a) as being unpatentable over Rose et al (US 5,770,843), further in view of Pierce (US 4,485,300 of record).

Claim 44 rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of US Patent No. 6,494,367. The examiner states that the scope of claim 31, 37-44 and 53 of the present application and claims 1 and 2 of US Patent No. 6,494,367 are practically identical.

8. ARGUMENTS:

In my explanations I cite my previously granted patents US Pat. 6,494,367 and European patent EP 1221144, and my Canadian patent CA 2,381,807 pertaining to the same invention. This application (10/089,756) is intended to clarify my claims in US Pat. 6,494,367 to avoid potential infringement. In the light of the Office Action of June 19, 2003, I cancelled claims 31, 33, 34, 37-43 and claim 53. The remaining claims were amended and I provided explanations that clearly differentiate my invention from the teachings of ROSE and PIERCE. The attached claims are those rejected in the Office Action of November 17, 2003. My drawings (filed 29th July, 2003, identical to those in my US Patent 6,494,367) were accepted.

Re: US Patent 5,770,843 (ROSE et al.):

In contrast to my invention, here's how the ROSE system works:

1. The multi-application card (MAC) is swiped at a card reader. The card reader reads the MAC identification number. That's where the similarity ends.

2. The MAC number is sent to the remote system. It reads the record, searches all the sub-records (or entries) for account numbers in the record and displays ALL accounts on a screen for the user to select one.

3. With all accounts on the MAC displayed - before having to enter anything - the user chooses one of the accounts, e.g. a Bank of America (BofA) Debit card.

4. The system now asks for the PIN of the BofA Debit card. The user enters the PIN for the BofA Debit card at a data entry device.

5. The PIN is sent to the remote system. If the PIN (which can be the same for ALL the accounts) matches that of the BofA Debit card, the transaction is allowed to proceed.

Differences between ROSE and the current Invention:

Here are important differences between my invention and that of ROSE et al.:

ROSE uses PINs, which (in over 90% of cases) are found to be the same for all accounts of a card owner, while my invention uses Index Numbers which must be unique for each account, enforcing better security.

ROSE discloses to a potential thief ALL the accounts on a MAC record by merely swiping the MAC at a point-of-service terminal - even *before* the user is asked to enter anything. As a result, any user (including a thief) could never make a mistake in selecting an account - because ALL accounts are shown and the user selects from among them. If there are 5 accounts on the MAC, in the ROSE invention, only 5 accounts are displayed and the user has 5 possible choices. In my invention (assuming 4 digits are used for the Index/CIN), there are 10,000 possible numbers (0000 to 9999) that the user could enter. Of the 10,000 possible numbers, typically more than 99.9% would be incorrect. Only the owner would know what accounts are on the MAC and the *unique* Index Number pertaining to each account.

Credit cards do not use PINs. In the ROSE system, if the MAC database uses the *same* PIN as the card issuer, a thief with a Multi-Application Card could simply swipe the MAC and select a credit card - which has no PIN - to use it.

Let us assume the ROSE invention forces a PIN on all cards including credit cards. Again, the thief sees all the accounts on the MAC by merely swiping the MAC at a point-of-sale terminal. If the thief knows the PIN of any *one* card belonging to the MAC owner, inherent in the design and confirmed by industry statistics, the thief could almost certainly use *all* the accounts on the MAC. Ironically, the ROSE invention would *help* a thief by displaying all the card accounts on the MAC, by simply swiping it at a point of sale. My invention requires the user to enter the index/CIN of a valid card account *without displaying* what accounts are on the MAC. Even if a thief learns the index/CIN of an account, s/he would be able to access only that one account on the MAC.

The ROSE invention requires and shows multiple exchanges of messages between the card reader and the database to identify a specific account number. By using unique index numbers for each stored account, my invention requires just one exchange of messages to identify a specific account number. This is extremely important because even milliseconds matter when it comes to card authorization.

The ROSE invention was designed for a kiosk; it requires a device that can display all accounts on the record so that a user can select from among them. My invention does not require such a device; it can use a standard debit card keypad.

Changes in account numbers (whether in ROSE or my invention) would require a change to both databases - the card issuer database and the MAC database. However, in the ROSE invention - unless the MAC uses a different PIN from that in the card issuer database - a change in the PIN of any account would require a change in the database of the card issuer and also a change to the PIN in the MAC database. In my invention, changes to CINs and PINs are independent of each other. If the MAC owner changes the index number (or CIN) of an account, no change is required to the issuer's database. If

the MAC owner changes the PIN of a card, the only database needing the change is the issuer database. Since the MAC database in my invention does not use PINs related to account numbers, no change is required to it.

In the ROSE invention, it is NOT possible to *identify* an account number using the MAC Number and the PIN because multiple accounts have the same PIN. In ROSE, the PIN is used to merely *confirm* a previously-selected (and already identified) account number. In my invention, the two data items, i.e. the MAC Number and the Index, are sufficient to *identify* an individual account number.

I believe use of the words "identify" and "single account number" in my claims differentiates this invention from ROSE. The Committee of 3 Examiners at the European Patent Office (Euro. Pat. EP 1221144) acknowledges the difference and so does the Canadian Intellectual Property Office. The USPTO Examiner of this application had also acknowledged the difference and sought rewording of the claims to reflect the difference. Therefore, as in my Canadian patent CA 2,381,807, I amended my claims to state that the data identification number and the index number identify "a *single* account number", clearly different from the teachings of ROSE and PIERCE. So it surprised me greatly when the claims were finally rejected.

Differences between PIERCE and the current Invention:

Here are important differences between my invention and that of PIERCE:

PIERCE describes a system that re-directs data from the retailer subsystem to the appropriate card issuer subsystem. The use of a card translator subsystem to translate (without additional input) an identification number and index number to a single account number is not in the teachings of either PIERCE or ROSE.

The claims in this patent application point out, as shown in Figure 6 of the drawings, that a card translator (a subsystem to convert a MAC number and index number to a single account number) may be located in, or connected to, a client/retailer subsystem, an issuer subsystem or an intermediate subsystem usually referred to in the industry as a card processor.

As stated earlier, I believe using the words "identify" and "single account number" in my claims differentiates this invention from ROSE and PIERCE. I had previously amended my claims to state that the data identification number and the index number identify a *single* account number, clearly different from the teachings of ROSE and PIERCE.

Double Patenting:

Claim 44 was rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of US Patent No. 6,494,367. Claims 31, 37-43 and 53 were previously cancelled. However, I understand from the Examiner that there is a means of linking Claim 44 with US Patent 6,494,367 so that they are linked together and cannot be sold separately. I am open to this type of resolution.

9. APPENDIX

CLAIMS

28. A system allowing a single card device to be utilized in accessing a plurality of applications, the system comprising:

    (a) a card processing system;
    (b) a card reader communicatively coupleable to the card processing system, the card reader being operative to read a data identification number from the single card device and to receive an index number selected by a user of the card device through a data interface;
    (c) the processing system, in response to receiving the data identification number and said index number from the card reader, being operative to identify a single account number associated with the data identification number and said index number when the index number is within a first subset of index numbers from a domain of potential index numbers.

29. The system of Claim 28, wherein the processing system, in response to receiving the data identification number and said index number from the card reader, is operative to disable the card device from further use when the index number is within a second subset of index numbers from the domain of potential index numbers.

30. The system of Claim 28, wherein the processing system, in response to receiving the data identification number and said index number from the card reader, is operative to re-enable a disabled card device when the index number is within a third subset of index numbers from the domain of potential index numbers.

32. A system using a single card device to access a plurality of applications, comprising:

a) at least one card issuer subsystem;

b) at least one card translator subsystem;

c) a client subsystem, comprising:

i. a card reader, capable of reading data including at least an identification number from the card device;

ii. a data entry means;

iii. means to:

1. read data including at least the identification number from the card device;

2. accept an index number pertaining to a single account number using the data entry means;

3. send a request to retrieve the account number, said request comprising the identification number and the index number, to a card translator subsystem;

4. receive a response comprising the account number from the subsystem to which the request was sent.

35. The system of claim 32, wherein the request is sent to a card processor subsystem that is operative to receive the request from any subsystem, process the request to determine that a card translator subsystem should receive the request, and transmit the request to the card translator subsystem.

36. The system of claim 32, wherein the request is sent to a card issuer subsystem that is operative to receive the request from any subsystem, process the request to determine that a card translator subsystem should receive the request, and transmit the request to the card translator subsystem.

44. The system of claim 32, wherein the card translator subsystem is communicatively coupleable to a system from the group comprising a client subsystem, a card processor subsystem and a card issuer subsystem.

45. A method for secure processing of multi-application card transactions, comprising the steps of:

a) reading data including at least an identification number from a card device;

b) accepting an index number, pertaining to a single account number, using a data entry means;

c) sending a request to retrieve a single account number, said request comprising the identification number, and the index number, to a card translator subsystem;

d) receiving account information comprising the single account number from the subsystem to which the request was sent.

46. The method of claim 45, further including sending the request to a card processor subsystem that is operative to receive the request from any subsystem, process the request to determine

that the card translator subsystem should receive the request, and transmit the request to the card translator subsystem.

47. The method of claim 45, further including sending the request from a card processor subsystem that is operative to initiate the request comprising an identification number and an index number, to the card translator subsystem.

48. The method of claim 45, further including sending the request to a card issuer subsystem that is operative to receive the request from any subsystem, process the request to determine that the card translator subsystem should receive the request, and transmit the request to the card translator subsystem.

49. The method of claim 45, further including sending the request from a card issuer subsystem that is operative to initiate the request comprising an identification number and an index number, to the card translator subsystem.

50. A method allowing a single card device to be utilized in accessing a plurality of applications, the method comprising the steps of:

a. reading a data identification number from the single card device;
b. receiving an index number selected by a user of the card device through a data interface;
c. identifying a single account number associated with the data identification number and said index number when the index number is within a first subset of index numbers from a domain of potential index numbers.

51. The method of claim 50, further including disabling the card device from further use when the index number is within a second subset of index numbers from the domain of potential index numbers.

52. The method of claim 50, further including re-enabling a disabled card device when the index number is within a third subset of index numbers from the domain of potential index numbers.

32 Merlin Drive, Brampton, ON, L6P 1G1, Canada
Tel: (905) 794-2752 – Fax: (905) 794-1411
Email: ajitzac@rogers.com

April 2, 2004

Applicant	:	Ajit K. Zacharias
Appl. No.	:	10/089,756
I.A. Filing Date	:	October 4, 2000
Priority Date	:	October 15, 1999
Title	:	Secure Multi-Application Card System
Grp. Art Unit	:	2876
Examiner	:	Mr. Seung H. Lee
Docket No.	:	AZSI-P-010

Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Re: Appeal Brief pertaining to Notice of Appeal filed February 6, 2004

Dear Sir/Madam:

This Appeal Brief is submitted in support of my Notice of Appeal filed February 6, 2004 in response to the Office Action of November 17, 2003. I attach the form PTO-2038 authorizing payment of the fee of $ 165.00 (small entity) for filing a brief in support of an Appeal.

If you have any questions, kindly contact me by phone at (905) 794-2752, or email me at ajitzac@rogers.com. Thank you.

Sincerely,

A. K. Zacharias

Ajit K. Zacharias
Sole Inventor and Applicant

APPEAL BRIEF

1. REAL PARTY OF INTEREST:

The Applicant. Not represented by a registered practitioner.

2. RELATED APPEALS AND INTERFERENCES:

None.

3. STATUS OF CLAIMS:

Claims 1-27, 31, 33, 34, 37-43 and Claim 53 were previously cancelled.

Claims 28-30, 32, 35, 36 and 44-52 were previously amended.

4. STATUS OF AMENDMENTS:

No amendments filed subsequent to final rejection.

5. SUMMARY OF THE INVENTION:

The invention is a multi-application card (MAC) system for providing card owners secure access to multiple card (and other) accounts. Since each account could involve access to a different application, it is termed a multi-application card.

A number of attempts have been made to implement a multi-application card system. A major difficulty with implementing such a system is that introducing a completely different hardware technology to implement a multi-application card system would necessitate changing the entire global equipment infrastructure for card processing, making it infeasible. That difficulty is overcome by the present invention. In this invention, a standard magnetic-stripe, smart or bar-coded card is used to access a database containing multiple account numbers, each identified by a unique index number (or code). This allows a MAC owner to carry one card but have use of multiple cards that s/he needs to carry for financial or non-financial applications.

The system comprises a MAC (with a machine-readable number corresponding to the MAC), a database (ideally located remote from the card) and a translator that uses the database to convert the MAC number to the account number the owner wishes to use.

The database correlates the MAC number with a record containing a list of card account numbers, each having a unique index number associated with it. The translator receives a request to convert the MAC number (read from the multi-application card) to the account number, using a manually entered index number (also called a Card Identification Number or CIN). The translator uses the received MAC number to access the corresponding record in the database. **Because each account number is assigned a unique index number within the record,** the translator is able to use the received index number to immediately identify and retrieve the corresponding account number and its associated security information, e.g. expiry date.

To avoid confusion in terminology such as "MAC Number", "Index Number", "PIN", "Card Identification Number" and "Account Number", here are the definitions of terms used in my application and the explanation:

Each Multi-Application Card (MAC) has a number. This is referred to in the following explanation as a "MAC number". The MAC number is read from the MAC by a card reader device.

Each MAC number corresponds to a record in the database. Each record in the database contains sub-records. Locating a specific sub-record in the database requires the MAC Number (to identify the record) and an Index Number (also referred to as a Card Identification Number or CIN) to identify the sub-record within it. The Index Number, typically a 4-digit number, is physically entered at a data entry device such as a keypad.

Most credit and debit card users are familiar with the use of a Personal Identification Number (PIN), which has served to verify the owner of a debit card. A PIN is also typically a 4-digit number, physically entered at a data entry device such as a keypad. Card industry research shows that over 90% of card owners use the same PIN for ALL their Debit, Check, ATM and Convenience cards. This seems logical because a PIN identifies the person, not the card. Credit cards are verified by signature and do not use PINS, making them more prone to fraudulent use.

My invention identifies three categories of index numbers, based on the content of the sub-records they relate to. Within the record, each sub-record identified by index numbers referred to as a "first subset" of index numbers, contains (or points to) a single account number. The account number could be a credit card number, a debit card number, driver's license number, etc. Within the same record, each sub-record identified by index numbers referred to as the "second subset" of index numbers, contains (or points to, or functions as) a LOCK code instead of an account number. Within the same record, each sub-record identified by index numbers referred to as the "third subset" of index numbers, contains (or points to, or functions as) an UNLOCK code, instead of an account number or a LOCK code.

Here are the steps involved in using my invention:

1. The multi-application card (MAC) is read at a card reader. The card reader reads the MAC number.

2. As when using a debit card, the user is asked to physically enter a number in the keypad. The user manually enters a number (called an Index Number or Card Identification Number).

3. The MAC Number and the Index Number are sent from the point-of-service to the card translator system. Using the MAC number, the translator locates a record in its database. The index number (or Card Identification Number) is used to find a sub-record (or entry) within the record. If, as the claim reads, the index number is within the *first* subset of index numbers (i.e. the sub-record identifies or contains a single account number), *that* account number is retrieved and processing continues. The account number could be a credit card number, a debit card number or some other account number. If the index number is within the *second* subset of index numbers (i.e. the sub-record identifies or contains a Lock code instead of an account number), the entire record is flagged as "locked" or "disabled". The MAC can no longer be used to access an account number from the database until the lock flag is removed. If the index number is within the *third* subset of index numbers (i.e. the sub-record identifies or contains an Unlock code instead of an account number or Lock code), the Lock flag for the record is removed, effectively "unlocking" or "re-enabling" the MAC.

The translator then transmits the card account number and other security information back to the sub-system, or program, that requested the translation of the MAC number to the actual account number. Although, in the preferred embodiment, the database and translator reside remote from the card, they could reside on the MAC, within the client subsystem, at the card issuer's system or any point within the network that makes up the Client-Server system.

6. ISSUES:

The Examiner rejects my claim that the PIN in the Rose invention (US 5,770,843) and the CIN in my invention are different. The difference in PIN and CIN, the processing steps and the resulting improvements are readily recognized by those ordinarily skilled in the art as well as Examiners at the European Patent Office and the Canadian Intellectual Property Office, which have granted me patents EP 1221144, and CA 2,381,807 respectively. For some reason the Examiner at the USPTO does not accept the difference. For instance, Claims 28c and 50c specifically claim sufficiency of the MAC Identification Number and the Index Number to identify a single account number. This is neither possible nor claimed in the ROSE invention, yet these claims have been rejected.

I applied for patents at the USPTO in two forms, directly and through the PCT. When the direct US patent was granted, I was compelled to accept narrow claims or have the entire patent denied; I accepted the narrow claims, because I felt I could explain the difference better during the US National Phase of my PCT application with the additional evidence of improvements on the basis of recognition by Examiners in the PCT countries. The narrow claims leave the patent vulnerable to infringement by minor variations. I do not believe this was the intention of the founding fathers of the United States when they instituted the concept of patents. It runs totally counter to the spirit of US Patent Law.

7. GROUPING OF CLAIMS:

Claims 28-30 and 50-52 rejected under U.S.C. 103(a) as being unpatentable over Rose et al (US 5,770,843 of record).

Claims 32, 35, 36 and 45-49 rejected under U.S.C. 103(a) as being unpatentable over Rose et al (US 5,770,843), further in view of Pierce (US 4,485,300 of record).

Claim 44 rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of US Patent No. 6,494,367. The examiner states that the scope of claim 31, 37-44 and 53 of the present application and claims 1 and 2 of US Patent No. 6,494,367 are practically identical.

8. ARGUMENTS:

In my explanations I cite my previously granted patents US Pat. 6,494,367 and European patent EP 1221144, and my Canadian patent CA 2,381,807 pertaining to the same invention. This application (10/089,756) is intended to clarify my claims in US Pat. 6,494,367 to avoid potential infringement. In the light of the Office Action of June 19, 2003, I cancelled claims 31, 33, 34, 37-43 and claim 53. The remaining claims were amended and I provided explanations that clearly differentiate my invention from the teachings of ROSE and PIERCE. The attached claims are those rejected in the Office Action of November 17, 2003. My drawings (filed 29th July, 2003, identical to those in my US Patent 6,494,367) were accepted.

Re: US Patent 5,770,843 (ROSE et al.):

In contrast to my invention, here's how the ROSE system works:

1. The multi-application card (MAC) is swiped at a card reader. The card reader reads the MAC identification number. That's where the similarity ends.

2. The MAC number is sent to the remote system. It reads the record, searches all the sub-records (or entries) for account numbers in the record and displays ALL accounts on a screen for the user to select one.

3. With all accounts on the MAC displayed - before having to enter anything - the user chooses one of the accounts, e.g. a Bank of America (BofA) Debit card.

4. The system now asks for the PIN of the BofA Debit card. The user enters the PIN for the BofA Debit card at a data entry device.

5. The PIN is sent to the remote system. If the PIN (which can be the same for ALL the accounts) matches that of the BofA Debit card, the transaction is allowed to proceed.

Differences between ROSE and the current Invention:

Here are important differences between my invention and that of ROSE et al.:

ROSE uses PINs, which (in over 90% of cases) are found to be the same for all accounts of a card owner, while my invention uses Index Numbers which must be unique for each account, enforcing better security.

ROSE discloses to a potential thief ALL the accounts on a MAC record by merely swiping the MAC at a point-of-service terminal - even *before* the user is asked to enter anything. As a result, any user (including a thief) could never make a mistake in selecting an account - because ALL accounts are shown and the user selects from among them. If there are 5 accounts on the MAC, in the ROSE invention, only 5 accounts are displayed and the user has 5 possible choices. In my invention (assuming 4 digits are used for the Index/CIN), there are 10,000 possible numbers (0000 to 9999) that the user could enter. Of the 10,000 possible numbers, typically more than 99.9% would be incorrect. Only the owner would know what accounts are on the MAC and the *unique* Index Number pertaining to each account.

Credit cards do not use PINs. In the ROSE system, if the MAC database uses the *same* PIN as the card issuer, a thief with a Multi-Application Card could simply swipe the MAC and select a credit card - which has no PIN - to use it.

Let us assume the ROSE invention forces a PIN on all cards including credit cards. Again, the thief sees all the accounts on the MAC by merely swiping the MAC at a point-of-sale terminal. If the thief knows the PIN of any *one* card belonging to the MAC owner, inherent in the design and confirmed by industry statistics, the thief could almost certainly use *all* the accounts on the MAC. Ironically, the ROSE invention would *help* a thief by displaying all the card accounts on the MAC, by simply swiping it at a point of sale. My invention requires the user to enter the index/CIN of a valid card account *without displaying* what accounts are on the MAC. Even if a thief learns the index/CIN of an account, s/he would be able to access only that one account on the MAC.

The ROSE invention requires and shows multiple exchanges of messages between the card reader and the database to identify a specific account number. By using unique index numbers for each stored account, my invention requires just one exchange of messages to identify a specific account number. This is extremely important because even milliseconds matter when it comes to card authorization.

The ROSE invention was designed for a kiosk; it requires a device that can display all accounts on the record so that a user can select from among them. My invention does not require such a device; it can use a standard debit card keypad.

Changes in account numbers (whether in ROSE or my invention) would require a change to both databases - the card issuer database and the MAC database. However, in the ROSE invention - unless the MAC uses a different PIN from that in the card issuer database - a change in the PIN of any account would require a change in the database of the card issuer and also a change to the PIN in the MAC database. In my invention, changes to CINs and PINs are independent of each other. If the MAC owner changes the index number (or CIN) of an account, no change is required to the issuer's database. If

the MAC owner changes the PIN of a card, the only database needing the change is the issuer database. Since the MAC database in my invention does not use PINs related to account numbers, no change is required to it.

In the ROSE invention, it is NOT possible to *identify* an account number using the MAC Number and the PIN because multiple accounts have the same PIN. In ROSE, the PIN is used to merely *confirm* a previously-selected (and already identified) account number. In my invention, the two data items, i.e. the MAC Number and the Index, are sufficient to *identify* an individual account number.

I believe use of the words "identify" and "single account number" in my claims differentiates this invention from ROSE. The Committee of 3 Examiners at the European Patent Office (Euro. Pat. EP 1221144) acknowledges the difference and so does the Canadian Intellectual Property Office. The USPTO Examiner of this application had also acknowledged the difference and sought rewording of the claims to reflect the difference. Therefore, as in my Canadian patent CA 2,381,807, I amended my claims to state that the data identification number and the index number identify "a *single* account number", clearly different from the teachings of ROSE and PIERCE. So it surprised me greatly when the claims were finally rejected.

Differences between PIERCE and the current Invention:

Here are important differences between my invention and that of PIERCE:

PIERCE describes a system that re-directs data from the retailer subsystem to the appropriate card issuer subsystem. The use of a card translator subsystem to translate (without additional input) an identification number and index number to a single account number is not in the teachings of either PIERCE or ROSE.

The claims in this patent application point out, as shown in Figure 6 of the drawings, that a card translator (a subsystem to convert a MAC number and index number to a single account number) may be located in, or connected to, a client/retailer subsystem, an issuer subsystem or an intermediate subsystem usually referred to in the industry as a card processor.

As stated earlier, I believe using the words "identify" and "single account number" in my claims differentiates this invention from ROSE and PIERCE. I had previously amended my claims to state that the data identification number and the index number identify a *single* account number, clearly different from the teachings of ROSE and PIERCE.

Double Patenting:

Claim 44 was rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of US Patent No. 6,494,367. Claims 31, 37-43 and 53 were previously cancelled. However, I understand from the Examiner that there is a means of linking Claim 44 with US Patent 6,494,367 so that they are linked together and cannot be sold separately. I am open to this type of resolution.

9. APPENDIX

CLAIMS

28. A system allowing a single card device to be utilized in accessing a plurality of applications, the system comprising:

(a) a card processing system;
(b) a card reader communicatively coupleable to the card processing system, the card reader being operative to read a data identification number from the single card device and to receive an index number selected by a user of the card device through a data interface;
(c) the processing system, in response to receiving the data identification number and said index number from the card reader, being operative to identify a single account number associated with the data identification number and said index number when the index number is within a first subset of index numbers from a domain of potential index numbers.

29. The system of Claim 28, wherein the processing system, in response to receiving the data identification number and said index number from the card reader, is operative to disable the card device from further use when the index number is within a second subset of index numbers from the domain of potential index numbers.

30. The system of Claim 28, wherein the processing system, in response to receiving the data identification number and said index number from the card reader, is operative to re-enable a disabled card device when the index number is within a third subset of index numbers from the domain of potential index numbers.

32. A system using a single card device to access a plurality of applications, comprising:

a) at least one card issuer subsystem;

b) at least one card translator subsystem;

c) a client subsystem, comprising:

i. a card reader, capable of reading data including at least an identification number from the card device;

ii. a data entry means;

iii. means to:

1. read data including at least the identification number from the card device;

2. accept an index number pertaining to a single account number using the data entry means;

3. send a request to retrieve the account number, said request comprising the identification number and the index number, to a card translator subsystem;

4. receive a response comprising the account number from the subsystem to which the request was sent.

35. The system of claim 32, wherein the request is sent to a card processor subsystem that is operative to receive the request from any subsystem, process the request to determine that a card translator subsystem should receive the request, and transmit the request to the card translator subsystem.

36. The system of claim 32, wherein the request is sent to a card issuer subsystem that is operative to receive the request from any subsystem, process the request to determine that a card translator subsystem should receive the request, and transmit the request to the card translator subsystem.

44. The system of claim 32, wherein the card translator subsystem is communicatively coupleable to a system from the group comprising a client subsystem, a card processor subsystem and a card issuer subsystem.

45. A method for secure processing of multi-application card transactions, comprising the steps of:

a) reading data including at least an identification number from a card device;

b) accepting an index number, pertaining to a single account number, using a data entry means;

c) sending a request to retrieve a single account number, said request comprising the identification number, and the index number, to a card translator subsystem;

d) receiving account information comprising the single account number from the subsystem to which the request was sent.

46. The method of claim 45, further including sending the request to a card processor subsystem that is operative to receive the request from any subsystem, process the request to determine

that the card translator subsystem should receive the request, and transmit the request to the card translator subsystem.

47. The method of claim 45, further including sending the request from a card processor subsystem that is operative to initiate the request comprising an identification number and an index number, to the card translator subsystem.

48. The method of claim 45, further including sending the request to a card issuer subsystem that is operative to receive the request from any subsystem, process the request to determine that the card translator subsystem should receive the request, and transmit the request to the card translator subsystem.

49. The method of claim 45, further including sending the request from a card issuer subsystem that is operative to initiate the request comprising an identification number and an index number, to the card translator subsystem.

50. A method allowing a single card device to be utilized in accessing a plurality of applications, the method comprising the steps of:

a. reading a data identification number from the single card device;
b. receiving an index number selected by a user of the card device through a data interface;
c. identifying a single account number associated with the data identification number and said index number when the index number is within a first subset of index numbers from a domain of potential index numbers.

51. The method of claim 50, further including disabling the card device from further use when the index number is within a second subset of index numbers from the domain of potential index numbers.

52. The method of claim 50, further including re-enabling a disabled card device when the index number is within a third subset of index numbers from the domain of potential index numbers.

32 Merlin Drive, Brampton, ON, L6P 1G1, Canada
Tel: (905) 794-2752 – Fax: (905) 794-1411
Email: ajitzac@rogers.com

April 2, 2004

Applicant	:	Ajit K. Zacharias
Appl. No.	:	10/089,756
I.A. Filing Date	:	October 4, 2000
Priority Date	:	October 15, 1999
Title	:	Secure Multi-Application Card System
Grp. Art Unit	:	2876
Examiner	:	Mr. Seung H. Lee
Docket No.	:	AZSI-P-010

Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Re: Appeal Brief pertaining to Notice of Appeal filed February 6, 2004

Dear Sir/Madam:

This Appeal Brief is submitted in support of my Notice of Appeal filed February 6, 2004 in response to the Office Action of November 17, 2003. I attach the form PTO-2038 authorizing payment of the fee of $ 165.00 (small entity) for filing a brief in support of an Appeal.

If you have any questions, kindly contact me by phone at (905) 794-2752, or email me at ajitzac@rogers.com. Thank you.

Sincerely,

A. K. Zacharias

Ajit K. Zacharias
Sole Inventor and Applicant

APPEAL BRIEF

1. REAL PARTY OF INTEREST:

The Applicant. Not represented by a registered practitioner.

2. RELATED APPEALS AND INTERFERENCES:

None.

3. STATUS OF CLAIMS:

Claims 1-27, 31, 33, 34, 37-43 and Claim 53 were previously cancelled.

Claims 28-30, 32, 35, 36 and 44-52 were previously amended.

4. STATUS OF AMENDMENTS:

No amendments filed subsequent to final rejection.

5. SUMMARY OF THE INVENTION:

The invention is a multi-application card (MAC) system for providing card owners secure access to multiple card (and other) accounts. Since each account could involve access to a different application, it is termed a multi-application card.

A number of attempts have been made to implement a multi-application card system. A major difficulty with implementing such a system is that introducing a completely different hardware technology to implement a multi-application card system would necessitate changing the entire global equipment infrastructure for card processing, making it infeasible. That difficulty is overcome by the present invention. In this invention, a standard magnetic-stripe, smart or bar-coded card is used to access a database containing multiple account numbers, each identified by a unique index number (or code). This allows a MAC owner to carry one card but have use of multiple cards that s/he needs to carry for financial or non-financial applications.

The system comprises a MAC (with a machine-readable number corresponding to the MAC), a database (ideally located remote from the card) and a translator that uses the database to convert the MAC number to the account number the owner wishes to use.

The database correlates the MAC number with a record containing a list of card account numbers, each having a unique index number associated with it. The translator receives a request to convert the MAC number (read from the multi-application card) to the account number, using a manually entered index number (also called a Card Identification Number or CIN). The translator uses the received MAC number to access the corresponding record in the database. **Because each account number is assigned a unique index number within the record,** the translator is able to use the received index number to immediately identify and retrieve the corresponding account number and its associated security information, e.g. expiry date.

To avoid confusion in terminology such as "MAC Number", "Index Number", "PIN", "Card Identification Number" and "Account Number", here are the definitions of terms used in my application and the explanation:

Each Multi-Application Card (MAC) has a number. This is referred to in the following explanation as a "MAC number". The MAC number is read from the MAC by a card reader device.

Each MAC number corresponds to a record in the database. Each record in the database contains sub-records. Locating a specific sub-record in the database requires the MAC Number (to identify the record) and an Index Number (also referred to as a Card Identification Number or CIN) to identify the sub-record within it. The Index Number, typically a 4-digit number, is physically entered at a data entry device such as a keypad.

Most credit and debit card users are familiar with the use of a Personal Identification Number (PIN), which has served to verify the owner of a debit card. A PIN is also typically a 4-digit number, physically entered at a data entry device such as a keypad. Card industry research shows that over 90% of card owners use the same PIN for ALL their Debit, Check, ATM and Convenience cards. This seems logical because a PIN identifies the person, not the card. Credit cards are verified by signature and do not use PINS, making them more prone to fraudulent use.

My invention identifies three categories of index numbers, based on the content of the sub-records they relate to. Within the record, each sub-record identified by index numbers referred to as a "first subset" of index numbers, contains (or points to) a single account number. The account number could be a credit card number, a debit card number, driver's license number, etc. Within the same record, each sub-record identified by index numbers referred to as the "second subset" of index numbers, contains (or points to, or functions as) a LOCK code instead of an account number. Within the same record, each sub-record identified by index numbers referred to as the "third subset" of index numbers, contains (or points to, or functions as) an UNLOCK code, instead of an account number or a LOCK code.

Here are the steps involved in using my invention:

1. The multi-application card (MAC) is read at a card reader. The card reader reads the MAC number.

2. As when using a debit card, the user is asked to physically enter a number in the keypad. The user manually enters a number (called an Index Number or Card Identification Number).

3. The MAC Number and the Index Number are sent from the point-of-service to the card translator system. Using the MAC number, the translator locates a record in its database. The index number (or Card Identification Number) is used to find a sub-record (or entry) within the record. If, as the claim reads, the index number is within the *first* subset of index numbers (i.e. the sub-record identifies or contains a single account number), *that* account number is retrieved and processing continues. The account number could be a credit card number, a debit card number or some other account number. If the index number is within the *second* subset of index numbers (i.e. the sub-record identifies or contains a Lock code instead of an account number), the entire record is flagged as "locked" or "disabled". The MAC can no longer be used to access an account number from the database until the lock flag is removed. If the index number is within the *third* subset of index numbers (i.e. the sub-record identifies or contains an Unlock code instead of an account number or Lock code), the Lock flag for the record is removed, effectively "unlocking" or "re-enabling" the MAC.

The translator then transmits the card account number and other security information back to the sub-system, or program, that requested the translation of the MAC number to the actual account number. Although, in the preferred embodiment, the database and translator reside remote from the card, they could reside on the MAC, within the client subsystem, at the card issuer's system or any point within the network that makes up the Client-Server system.

6. ISSUES:

The Examiner rejects my claim that the PIN in the Rose invention (US 5,770,843) and the CIN in my invention are different. The difference in PIN and CIN, the processing steps and the resulting improvements are readily recognized by those ordinarily skilled in the art as well as Examiners at the European Patent Office and the Canadian Intellectual Property Office, which have granted me patents EP 1221144, and CA 2,381,807 respectively. For some reason the Examiner at the USPTO does not accept the difference. For instance, Claims 28c and 50c specifically claim sufficiency of the MAC Identification Number and the Index Number to identify a single account number. This is neither possible nor claimed in the ROSE invention, yet these claims have been rejected.

I applied for patents at the USPTO in two forms, directly and through the PCT. When the direct US patent was granted, I was compelled to accept narrow claims or have the entire patent denied; I accepted the narrow claims, because I felt I could explain the difference better during the US National Phase of my PCT application with the additional evidence of improvements on the basis of recognition by Examiners in the PCT countries. The narrow claims leave the patent vulnerable to infringement by minor variations. I do not believe this was the intention of the founding fathers of the United States when they instituted the concept of patents. It runs totally counter to the spirit of US Patent Law.

7. GROUPING OF CLAIMS:

Claims 28-30 and 50-52 rejected under U.S.C. 103(a) as being unpatentable over Rose et al (US 5,770,843 of record).

Claims 32, 35, 36 and 45-49 rejected under U.S.C. 103(a) as being unpatentable over Rose et al (US 5,770,843), further in view of Pierce (US 4,485,300 of record).

Claim 44 rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of US Patent No. 6,494,367. The examiner states that the scope of claim 31, 37-44 and 53 of the present application and claims 1 and 2 of US Patent No. 6,494,367 are practically identical.

8. ARGUMENTS:

In my explanations I cite my previously granted patents US Pat. 6,494,367 and European patent EP 1221144, and my Canadian patent CA 2,381,807 pertaining to the same invention. This application (10/089,756) is intended to clarify my claims in US Pat. 6,494,367 to avoid potential infringement. In the light of the Office Action of June 19, 2003, I cancelled claims 31, 33, 34, 37-43 and claim 53. The remaining claims were amended and I provided explanations that clearly differentiate my invention from the teachings of ROSE and PIERCE. The attached claims are those rejected in the Office Action of November 17, 2003. My drawings (filed 29th July, 2003, identical to those in my US Patent 6,494,367) were accepted.

Re: US Patent 5,770,843 (ROSE et al.):

In contrast to my invention, here's how the ROSE system works:

1. The multi-application card (MAC) is swiped at a card reader. The card reader reads the MAC identification number. That's where the similarity ends.

2. The MAC number is sent to the remote system. It reads the record, searches all the sub-records (or entries) for account numbers in the record and displays ALL accounts on a screen for the user to select one.

3. With all accounts on the MAC displayed - before having to enter anything - the user chooses one of the accounts, e.g. a Bank of America (BofA) Debit card.

4. The system now asks for the PIN of the BofA Debit card. The user enters the PIN for the BofA Debit card at a data entry device.

5. The PIN is sent to the remote system. If the PIN (which can be the same for ALL the accounts) matches that of the BofA Debit card, the transaction is allowed to proceed.

Differences between ROSE and the current Invention:

Here are important differences between my invention and that of ROSE et al.:

ROSE uses PINs, which (in over 90% of cases) are found to be the same for all accounts of a card owner, while my invention uses Index Numbers which must be unique for each account, enforcing better security.

ROSE discloses to a potential thief ALL the accounts on a MAC record by merely swiping the MAC at a point-of-service terminal - even *before* the user is asked to enter anything. As a result, any user (including a thief) could never make a mistake in selecting an account - because ALL accounts are shown and the user selects from among them. If there are 5 accounts on the MAC, in the ROSE invention, only 5 accounts are displayed and the user has 5 possible choices. In my invention (assuming 4 digits are used for the Index/CIN), there are 10,000 possible numbers (0000 to 9999) that the user could enter. Of the 10,000 possible numbers, typically more than 99.9% would be incorrect. Only the owner would know what accounts are on the MAC and the *unique* Index Number pertaining to each account.

Credit cards do not use PINs. In the ROSE system, if the MAC database uses the *same* PIN as the card issuer, a thief with a Multi-Application Card could simply swipe the MAC and select a credit card - which has no PIN - to use it.

Let us assume the ROSE invention forces a PIN on all cards including credit cards. Again, the thief sees all the accounts on the MAC by merely swiping the MAC at a point-of-sale terminal. If the thief knows the PIN of any *one* card belonging to the MAC owner, inherent in the design and confirmed by industry statistics, the thief could almost certainly use *all* the accounts on the MAC. Ironically, the ROSE invention would *help* a thief by displaying all the card accounts on the MAC, by simply swiping it at a point of sale. My invention requires the user to enter the index/CIN of a valid card account *without displaying* what accounts are on the MAC. Even if a thief learns the index/CIN of an account, s/he would be able to access only that one account on the MAC.

The ROSE invention requires and shows multiple exchanges of messages between the card reader and the database to identify a specific account number. By using unique index numbers for each stored account, my invention requires just one exchange of messages to identify a specific account number. This is extremely important because even milliseconds matter when it comes to card authorization.

The ROSE invention was designed for a kiosk; it requires a device that can display all accounts on the record so that a user can select from among them. My invention does not require such a device; it can use a standard debit card keypad.

Changes in account numbers (whether in ROSE or my invention) would require a change to both databases - the card issuer database and the MAC database. However, in the ROSE invention - unless the MAC uses a different PIN from that in the card issuer database - a change in the PIN of any account would require a change in the database of the card issuer and also a change to the PIN in the MAC database. In my invention, changes to CINs and PINs are independent of each other. If the MAC owner changes the index number (or CIN) of an account, no change is required to the issuer's database. If

the MAC owner changes the PIN of a card, the only database needing the change is the issuer database. Since the MAC database in my invention does not use PINs related to account numbers, no change is required to it.

In the ROSE invention, it is NOT possible to *identify* an account number using the MAC Number and the PIN because multiple accounts have the same PIN. In ROSE, the PIN is used to merely *confirm* a previously-selected (and already identified) account number. In my invention, the two data items, i.e. the MAC Number and the Index, are sufficient to *identify* an individual account number.

I believe use of the words "identify" and "single account number" in my claims differentiates this invention from ROSE. The Committee of 3 Examiners at the European Patent Office (Euro. Pat. EP 1221144) acknowledges the difference and so does the Canadian Intellectual Property Office. The USPTO Examiner of this application had also acknowledged the difference and sought rewording of the claims to reflect the difference. Therefore, as in my Canadian patent CA 2,381,807, I amended my claims to state that the data identification number and the index number identify "a *single* account number", clearly different from the teachings of ROSE and PIERCE. So it surprised me greatly when the claims were finally rejected.

Differences between PIERCE and the current Invention:

Here are important differences between my invention and that of PIERCE:

PIERCE describes a system that re-directs data from the retailer subsystem to the appropriate card issuer subsystem. The use of a card translator subsystem to translate (without additional input) an identification number and index number to a single account number is not in the teachings of either PIERCE or ROSE.

The claims in this patent application point out, as shown in Figure 6 of the drawings, that a card translator (a subsystem to convert a MAC number and index number to a single account number) may be located in, or connected to, a client/retailer subsystem, an issuer subsystem or an intermediate subsystem usually referred to in the industry as a card processor.

As stated earlier, I believe using the words "identify" and "single account number" in my claims differentiates this invention from ROSE and PIERCE. I had previously amended my claims to state that the data identification number and the index number identify a *single* account number, clearly different from the teachings of ROSE and PIERCE.

Double Patenting:

Claim 44 was rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of US Patent No. 6,494,367. Claims 31, 37-43 and 53 were previously cancelled. However, I understand from the Examiner that there is a means of linking Claim 44 with US Patent 6,494,367 so that they are linked together and cannot be sold separately. I am open to this type of resolution.

9. APPENDIX

CLAIMS

28. A system allowing a single card device to be utilized in accessing a plurality of applications, the system comprising:

(a) a card processing system;
(b) a card reader communicatively coupleable to the card processing system, the card reader being operative to read a data identification number from the single card device and to receive an index number selected by a user of the card device through a data interface;
(c) the processing system, in response to receiving the data identification number and said index number from the card reader, being operative to identify a single account number associated with the data identification number and said index number when the index number is within a first subset of index numbers from a domain of potential index numbers.

29. The system of Claim 28, wherein the processing system, in response to receiving the data identification number and said index number from the card reader, is operative to disable the card device from further use when the index number is within a second subset of index numbers from the domain of potential index numbers.

30. The system of Claim 28, wherein the processing system, in response to receiving the data identification number and said index number from the card reader, is operative to re-enable a disabled card device when the index number is within a third subset of index numbers from the domain of potential index numbers.

32. A system using a single card device to access a plurality of applications, comprising:

a) at least one card issuer subsystem;

b) at least one card translator subsystem;

c) a client subsystem, comprising:

i. a card reader, capable of reading data including at least an identification number from the card device;

ii. a data entry means;

iii. means to:

1. read data including at least the identification number from the card device;

2. accept an index number pertaining to a single account number using the data entry means;

3. send a request to retrieve the account number, said request comprising the identification number and the index number, to a card translator subsystem;

4. receive a response comprising the account number from the subsystem to which the request was sent.

35. The system of claim 32, wherein the request is sent to a card processor subsystem that is operative to receive the request from any subsystem, process the request to determine that a card translator subsystem should receive the request, and transmit the request to the card translator subsystem.

36. The system of claim 32, wherein the request is sent to a card issuer subsystem that is operative to receive the request from any subsystem, process the request to determine that a card translator subsystem should receive the request, and transmit the request to the card translator subsystem.

44. The system of claim 32, wherein the card translator subsystem is communicatively coupleable to a system from the group comprising a client subsystem, a card processor subsystem and a card issuer subsystem.

45. A method for secure processing of multi-application card transactions, comprising the steps of:

a) reading data including at least an identification number from a card device;

b) accepting an index number, pertaining to a single account number, using a data entry means;

c) sending a request to retrieve a single account number, said request comprising the identification number, and the index number, to a card translator subsystem;

d) receiving account information comprising the single account number from the subsystem to which the request was sent.

46. The method of claim 45, further including sending the request to a card processor subsystem that is operative to receive the request from any subsystem, process the request to determine

that the card translator subsystem should receive the request, and transmit the request to the card translator subsystem.

47. The method of claim 45, further including sending the request from a card processor subsystem that is operative to initiate the request comprising an identification number and an index number, to the card translator subsystem.

48. The method of claim 45, further including sending the request to a card issuer subsystem that is operative to receive the request from any subsystem, process the request to determine that the card translator subsystem should receive the request, and transmit the request to the card translator subsystem.

49. The method of claim 45, further including sending the request from a card issuer subsystem that is operative to initiate the request comprising an identification number and an index number, to the card translator subsystem.

50. A method allowing a single card device to be utilized in accessing a plurality of applications, the method comprising the steps of:

a. reading a data identification number from the single card device;
b. receiving an index number selected by a user of the card device through a data interface;
c. identifying a single account number associated with the data identification number and said index number when the index number is within a first subset of index numbers from a domain of potential index numbers.

51. The method of claim 50, further including disabling the card device from further use when the index number is within a second subset of index numbers from the domain of potential index numbers.

52. The method of claim 50, further including re-enabling a disabled card device when the index number is within a third subset of index numbers from the domain of potential index numbers.

US 101015800BP1

Creation date: 04-15-2004
Indexing Officer: HLE18 - HOA LE
Team: OIPEBackFileIndexing
Dossier: 10101580

Legal Date: 04-13-2004

No.	Doccode	Number of pages
1	A.NE	3
2	CLM	7
3	REM	8

Total number of pages: 18

Remarks:

Order of re-scan issued on .....